Fig. 1

CONFIGURATION STORAGE

POSITION / ADDRESS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ROW (1)	1	1	1	0	1	0	1	1	0	0	0	1	0	1	1	1	1	0	0	1
ROW (2)	1	1	1	0	1	0	0	1	0	0	0	1	0	1	0	0	1	0	0	1
ROW (3)	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0

KEYS:
ROW (1): ORIGINAL CONFIGURATION-DATA SEQUENCE
ROW (2): ENCRYPTED CONFIGURATION-DATA SEQUENCE
ROW (3): SECRET SEQUENCE STORED IN NONVOLATILE STORAGE MEANS 22
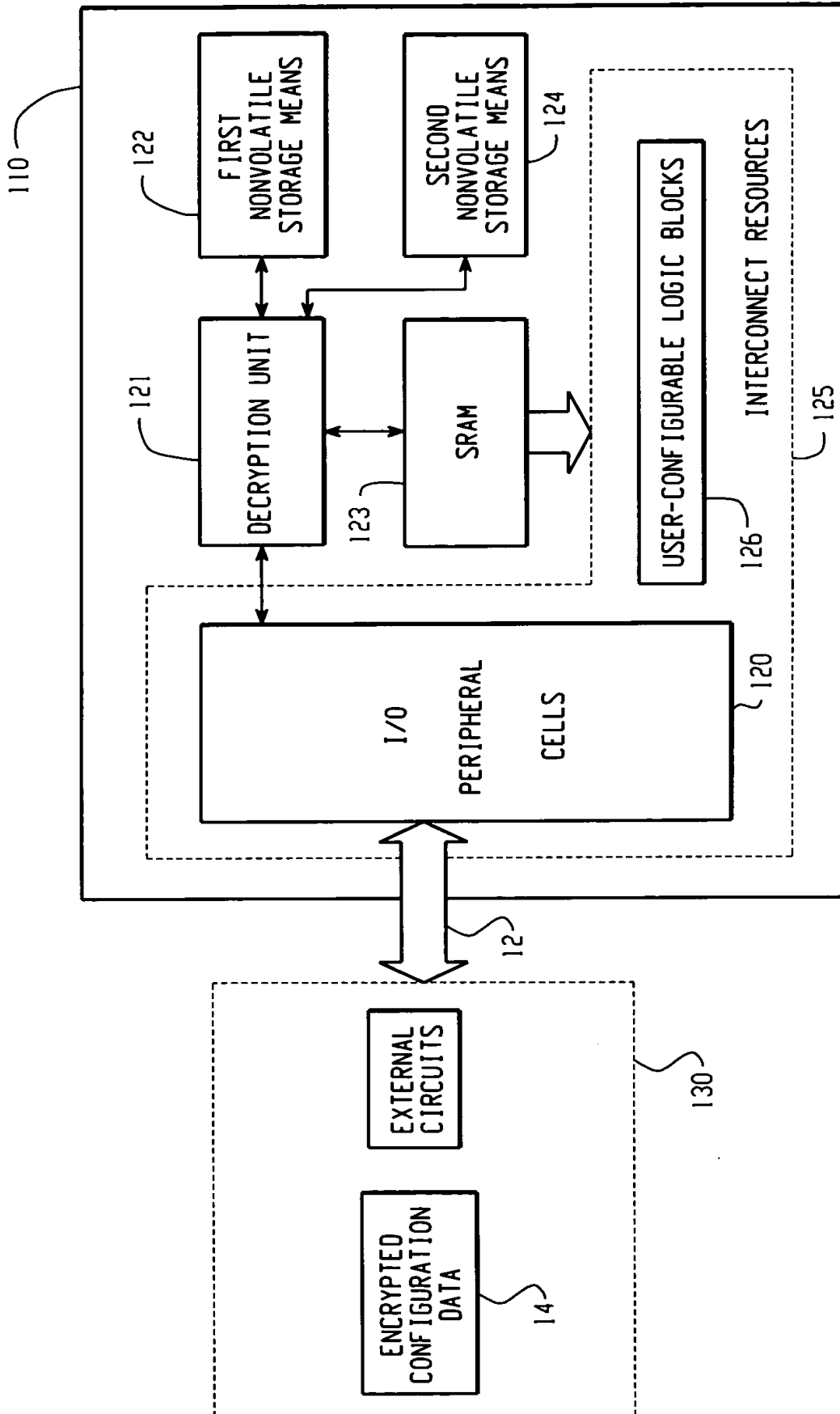POSITIONS 7 AND 14-16: BITS TO BE ENCRYPTED

Fig. 2

110

122 — FIRST NONVOLATILE STORAGE MEANS

124 — SECOND NONVOLATILE STORAGE MEANS

121 — DECRYPTION UNIT

123 — SRAM

126 — USER-CONFIGURABLE LOGIC BLOCKS

125 — INTERCONNECT RESOURCES

120 — I/O PERIPHERAL CELLS

12

130 — EXTERNAL CIRCUITS

14 — ENCRYPTED CONFIGURATION DATA

Fig. 3

4/7

CONFIG STORAGE

POSITION / ADDRESS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ROW (1)	1	1	1	0	1	0	1	1	0	0	1	0	0	1	1	1	1	0	0	1
ROW (2)	1	1	1	0	1	0	0	1	1	0	0	0	1	m_{14}	m_{15}	m_{16}	1	0	0	1
ROW (3)	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	0	0	0
ROW (4)	x	x	x	x	x	x	1	x	x	x	x	x	x	0	1	1	x	x	x	x

40

42 44 46 52 54

50 50 50

KEYS:
ROW (1): ORIGINAL CONFIGURATION-DATA SEQUENCE
ROW (2): ENCRYPTED CONFIGURATION-DATA SEQUENCE: $m_{14} \, m_{15} \, m_{16} \in \{000,001,010,100,101,110,111\}$
ROW (3): ADDRESS INFORMATION STORED IN THE FIRST NONVOLATILE STORAGE MEANS 122
ROW (4): OVERWRITE-DATA INFORMATION STORED IN THE SECOND NONVOLATILE STORAGE MEANS 124; X=DON'T CARE.
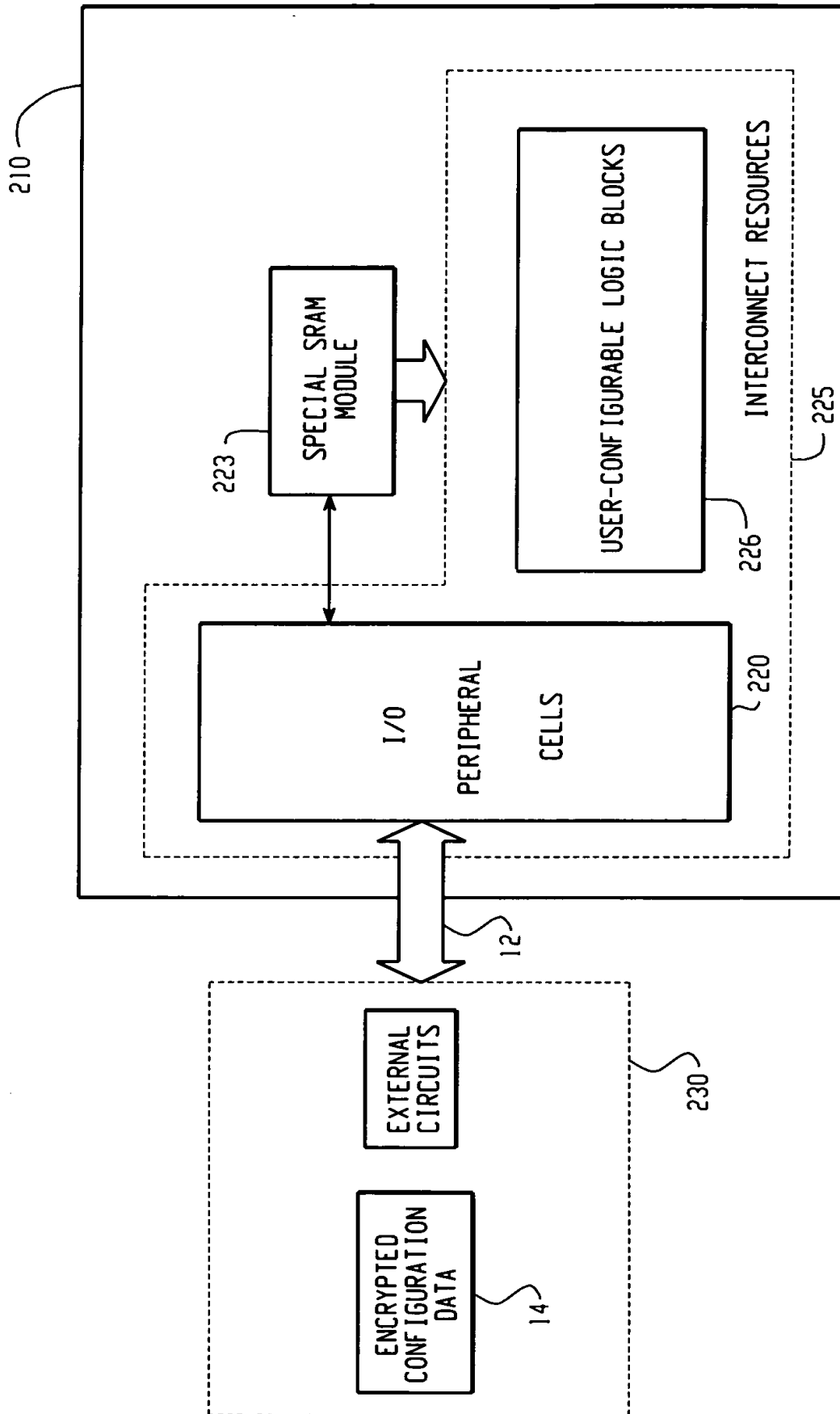POSITIONS 7 AND 14-16: BITS TO BE ENCRYPTED

Fig. 4

Fig. 5

POSITION/ADDRESS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ROW (1)	1	1	1	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	0	1
ROW (1)	1	1	1	0	1	0	0	1	1	0	0	0	1	m_{14}	m_{15}	m_{16}	1	0	0	1
ROW (1)	R/W	R/W	R/W	R/W	R/W	R/W	@1	R/W	R/W	R/W	R/W	R/W	R/W	@0	@1	@1	R/W	R/W	R/W	R/W

KEYS:
ROW (1): ORIGINAL CONFIGURATION-DATA SEQUENCE
ROW (2): ENCRYPTED CONFIGURATION-DATA SEQUENCE: m_{14} m_{15} m_{16} ∈ {000,001,010,100,101,110,111}
ROW (4): READ/WRITE STATUS OF THE SPECIAL SRAM MODULE 223; R/W=READ-AND-WRITE POSSIBLE; @=STICKING AT POSITIONS 7 AND 14-16; BITS TO BE ENCRYPTED

Fig. 6

7	~60
14	~60
15	~60
16	
EOL	~62
:	
:	
:	
:	

22 →

Fig. 7

(7, 1)	~60
(14, 0)	~60
(15, 1)	~60
(16, 1)	
EOL	~62
:	
:	
:	
:	

22 →

Fig. 8

(7, MODIFICATION, x)	~60
(14, OVERWRITE, 0)	~60
(15, MODIFICATION, x)	~60
(16, OVERWRITE, 1)	
EOL	~62
:	
:	
:	
:	

22 →

Fig. 9